UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/598,719	09/08/2006	Agostinho De Arruda Villela	2171323-000002	9289

44777 7590 10/15/2009
W. EDWARD RAMAGE
COMMERCE CENTER SUITE 1000
211 COMMERCE ST
NASHVILLE, TN 37201

EXAMINER	
WRIGHT, BRYAN F	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
10/15/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eramage@bakerdonelson.com

Office Action Summary	**Application No.** 10/598,719	**Applicant(s)** DE ARRUDA VILLELA, AGOSTINHO	
	Examiner BRYAN WRIGHT	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/28/2009 has been entered. Claims 17-35 are pending.

1. Claims 17-30, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chaung (US Patent Publication No. 2004/0039921) in view of Matsuzaki et al. (WO 2004/023275 and Matsuzaki hereinafter (cited from IDS)) and further in view of Drew (US Patent No. 6,477,645).

2. As to claims 17 and 35, Chaung teaches a method for identifying devices and controlling access to a service, comprising the steps of:

collecting data related to software and hardware configurations from a device through a software agent (i.e., ... teaches gathered basic client system information from the client 12 are then transferred to the server 14 for validation [par. 38]);

generating a digital signature for the device by hashing the software and hardware configuration data (i.e., ... teaches to generate hash values for each file, or asymmetric cryptographic functions to generate digital signatures for each file. The original version of the files as well as patches, updates/upgrades of all types of operating system or application software should be fingerprinted [par. 34]);

sending the digital signature of the device to an authentication server (i.e., … teaches transferred to the server 14 for validation [par. 38]);

Chaung does not expressly disclose:

determining whether the device has been excluded from accessing or enrolling in the service.

However at the time of applicant's original filing the device status verification was well known and would have been an obvious modification of Chaung as disclosed by Matsuzaki. Matsuzaki discloses:

determining whether the device has been excluded from accessing or enrolling in the service (to provide means to determine appropriate access conditions [S55-S58, fig. 9]).

Therefore, given Chaung ability to authenticate devices, a person having ordinary skill in the art would recognize the advantage of modifying Chaung to enhance device authentication with the well known feature of device management as disclosed by Matsuzaki.

The combination of Chaung in view of Matsuzaki does not expressly teach: the claim limitation element of a software agent is installed on the device

However, the use of a software agent was well known in the art at the time of applicant's original filing and would have a obvious modification of the teaching of Chaung in view of Matsuzaki as disclosed by Drews. Drews discloses:

a software agent is installed on the device (to provide software agent capability [col. 4, lines 15-20]).

Therefore given Chaung in view of Matsuzaki ability to authenticate devices, a person having ordinary skill in the art would recognize the advantage of modifying the teachings of Chaung in view of Matsuzaki to enhance device authentication with the well known feature of a software agent as disclosed by Drews.

3. As to claim 18, Chaung teaches a method where the digital signature sent to the authentication server is encrypted (e.g., secure)(i.e., ... teaches authentication data transferred to the server 14 for validation [par. 38]).

4. As to claim 19, although the teaching of Chaung in view of Matsuzaki discloses elements of the claimed invention, the combination does not disclose: A where the software agent is installed on the device as part of the process of using the device to access a service.

However, the use of a software agent was well known in the art at the time of applicant's original filing and would have a obvious modification of the teaching of Chaung in view of Matsuzaki as disclosed by Drews. Drews discloses:

where the software agent is installed on the device as part of the process of using the device to access a service (to provide software agent capability [col. 4, lines 15-20]).

Therefore given Chaung in view of Matsuzaki ability to authenticate devices, a person having ordinary skill in the art would recognize the advantage of modifying the teachings of Chaung in view of Matsuzaki to enhance device authentication with the well known feature of a software agent as disclosed by Drews.

5. As to claim 20, Chaung teaches a method where the hashes used to generate the digital signature are changed with every attempt to access a service, and the hashes cannot be reversed (e.g., one-way function/Hash) (i.e., ... teaches to generate hash values for each file, or asymmetric cryptographic functions to generate digital signatures for each file. The original version of the files as well as patches, updates/upgrades of all types of operating system or application software should be fingerprinted [par. 34]).

6. As to claim 21, Chaung teaches a method where the digital signature is one of several stages (i.e., bi-directional authentication) of a framework of authorization and authentication processes governing access to the service by the device [par. 37].

7. As to claim 22, Chaung teaches a method where the authentication server compares the digital signature sent with one or more previously-stored digital signatures (i.e., ... teaches transferred to the server 14 for validation [par. 38]).

8. As to claims 23-25, although Chaung illustrates elements of the claimed invention, Chaung does not disclose:

A method where the authentication server determines whether the device has been excluded from accessing or enrolling in the service by determining whether the device is on a list or in a group of devices not allowed to access the service, or is included within a group of devices allowed to access the service (claim 23).

A method where the authentication server allows a maximum number of enrollments for a particular device (claim 24).

A method where the maximum number of enrollments is zero (claim 25).

However at the time of applicant's original filing the device status verification was well known and would have been an obvious modification of Chaung as disclosed by Matsuzaki. Matsuzaki discloses:

A method where the authentication server determines whether the device has been excluded from accessing or enrolling in the service by determining whether the device is on a list or in a group of devices not allowed to access the service, or is included within a group of devices allowed to access the service (to provide (to provide means to determine appropriate access condition [S55-S58, fig. 9]) (claim 23).

A method where the authentication server allows a maximum number of enrollments for a particular device (to provide device registration management capability [pg. 14, lines 1-15])(claim 24).

A method where the maximum number of enrollments is zero (to provide device registration management capability [pg. 18, lines 20-25]) (claim 25).

Therefore, given Chaung ability to authenticate devices, a person having ordinary skill in the art would recognize the advantage of modifying Chaung to enhance device authentication with the well known feature of device management as disclosed by Matsuzaki.

9. As to claim 26, Chaung teaches a method where the authentication server allows minor modifications (e.g., updates) to the software or hardware configurations of a previously-enrolled device so as to preserve access or denial of access for the device [par. 34].

10. As to claim 27, Chaung teaches a method where the previously- stored digital signature of the device is updated to reflect the modifications (i.e., patches/upgrades [par. 34]).

11. As to claims 28-30, although Chaung illustrates elements of the claimed invention, Chaung does not disclose:

A method where the authentication server logs all accesses or attempted accesses by a device to the service (claim 28).

A method where multiple devices can be registered for a single user with the authentication server to create a registration hierarchy (claim 29).

A method where a user can unregister a device only through the device itself, or another device within the registration hierarchy registered earlier than the device to be unregistered (claim 30).

However at the time of applicant's original filing the device status verification was well known and would have been an obvious modification of Chaung as disclosed by Matsuzaki. Matsuzaki discloses:

A method where the authentication server logs all accesses or attempted accesses by a device to the service (to provide tracking means for devices access [pg. 23, lines 5-12] (claim 28).

A method where multiple devices (i.e., Id1, Id2...idN) can be registered for a single user with the authentication server to create a registration hierarchy (to provide the capability to maintain and track multiple devices [pg. 27, lines 5-10])(claim 29).

A method where a user can unregister a device only through the device itself, or another device within the registration hierarchy registered earlier than the device to be unregistered (to provide the capability to unregister a device [pg. 29, lines 5-15]) (claim 30).

Therefore, given Chaung ability to authenticate devices, a person having ordinary skill in the art would recognize the advantage of modifying Chaung to enhance device authentication with the well known feature of device management as disclosed by Matsuzaki.

12. Claims 31-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over IE020429 Abstract (cited from IDS) in view of Matsuzaki and further in view of Drews.

13. As to claim 31, IE020429 teaches a method for identifying devices and controlling access to a service (i.e., ...teaches developing measurements which uniquely identify a digital device or system based on their physical characteristics for the purpose of authenticating remote access providers [pg. 1]), comprising the steps of:

collecting (e.g., gathering) data related to software and hardware configurations from the device through a software agent (i.e., …teaches a method of gathering data related to the computer for purpose of verification [pg. 14]);

generating a digital signature for the device by hashing the software and hardware configuration data (i.e., …teaches a unique identification for a system can be readily obtained and input to a fingerprint creation process. …further teaches unique identity can be combined with intrinsic and private identity in a typical authentication scheme such as a hash [pg. 11]);

sending the digital signature of the device to the authentication server (i.e., …teaches sending said gathered first set of data to said identification server over said created first secure connection [pg. 14]);

IE020429 does not explicitly teach:

verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero,

and registering the device as authorized to access the service.

However at the time of applicant's original filing, device management was well known and would have been an obvious modification of IE020429 as disclosed by Matsuzaki. Matsuzaki discloses:

verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero (to provide the capability to determine if a device is un registered [pg. 18, lines 20-25]),

and registering the device as authorized to access the service (to provide the capability to register devices [pg. 19, lines 5-12]).

Therefore given IE020429's capability to authenticate a device, a person having ordinary skill in the art would recognize the advantage of modifying IE020429 to provide the capability to track devices in a network environment with the well known feature of device management as disclosed by Matsuzaki,

The combination of IE020429 in view of Matsuzaki does not expressly teach: the claim limitation element of a software agent installed on a device

However, the use of a software agent was well known in the art at the time of applicant's original filing and would have an obvious modification of the teaching of IE020429 in view of Matsuzaki as disclosed by Drews. Drews discloses:

a software agent installed on a device (to provide software agent capability [col. 4, lines 15-20]).

Therefore given IE020429 in view of Matsuzaki's ability to authenticate devices, a person having ordinary skill in the art would recognize the advantage of modifying the teachings of IE020429 in view of Matsuzaki to enhance device authentication with the well known feature of a software agent as disclosed by Drews.

14. As to claim 32, IE020429 teaches a method further comprising the step of verifying the identity of the device each time it subsequently attempts to access the service (i.e., teaches the measurements to be made must be determined prior to gathering the first identity and the identical measurements must be made every time the computer is to be identified (i.e., attempts access) [pg. 13]).

15. As to claim 33, IE020429 teaches a method where the step of verifying the identity of the device comprises the steps of:

collecting (e.g., gathering) data related to current software and hardware configurations from the device through a software agent (i.e., ...teaches a method of gathering data related to the computer for purpose of verification [pg. 14]);

generating a digital signature for the device by hashing the software and hardware configuration data (i.e., ...teaches a unique identification for a system can be readily obtained and input to a fingerprint creation process. ...further teaches unique identity can be combined with intrinsic and private identity in a typical authentication scheme such as a hash [pg. 11]);

sending the digital signature (i.e., gather first set) of the device to the authentication server (i.e., ...teaches sending said gathered first set of data to said identification server over said created first secure connection [pg. 14]);

and comparing the digital signature sent with one or more previously-stored digital signatures for the device [pg. 11].

IE020429 does not explicitly disclose the use of a software agent.
However, the use of a software agent was well known in the art at the time of applicant's original filing and would have a obvious modification of the teaching of IE020429 as disclosed by Drews. Drews discloses:

a software agent is installed on the device (to provide software agent capability [col. 4, lines 15-20]).

Therefore given IE020429's ability to authenticate devices, a person having ordinary skill in the art would recognize the advantage of modifying the teachings of IE020429 to enhance device authentication with the well known feature of a software agent as disclosed by Drews.

16. As to claim 34, IE020429 teaches a method where the step of verifying the identity of the device comprises the steps of:

collecting (e.g., gathering) data related to current software and hardware configurations from the device through a software agent (i.e., ...teaches a method of gathering data related to the computer for purpose of verification [pg. 14]);

generating a digital signature for the device by hashing the software and hardware configuration data (i.e., ...teaches a unique identification for a system can be readily obtained and input to a fingerprint creation process. ...further teaches unique identity can be combined with intrinsic and private identity in a typical authentication scheme such as a hash [pg. 11]);

sending the digital signature (e.g., first set)of the device to the authentication server (i.e., ...teaches sending said gathered first set of data to said identification server over said created first secure connection [pg. 14]);

IE020429 does not explicitly teach:

verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero, However at the time of applicant's original filing, device management was well known and would have been an obvious modification of IE020429 as disclosed by Matsuzaki. Matsuzaki discloses:

verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero (to provide the capability to determine if a device is un registered [pg. 18, lines 20-25]),

Therefore given IE020429's capability to authenticate a device, a person having ordinary skill in the art would recognize the advantage of modifying IE020429 to provide the capability to track devices in a network environment with the well known feature of device management as disclosed by Matsuzaki,

The combination of IE020429 in view of Matsuzaki does not expressly teach: the claim limitation element of a software agent installed on a device

However, the use of a software agent was well known in the art at the time of applicant's original filing and would have an obvious modification of the teachings of IE020429 in view of Matsuzaki as disclosed by Drews. Drews discloses:

a software agent installed on a device (to provide software agent capability [col. 4, lines 15-20]).

Therefore given IE020429 in view of Matsuzaki's ability to authenticate devices, a person having ordinary skill in the art would recognize the advantage of modifying the teachings of IE020429 in view of Matsuzaki to enhance device authentication with the well known feature of a software agent as disclosed by Drews.

Prior Art Made of Record

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Patent No. 6,330,588

b. Patent Publication No. 2003/0208569

c. Patent No. 6,148,401

.

Response to Arguments

Applicant's arguments with respect to claims 17-35 have been considered but are moot in view of the new ground(s) of rejection.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431